Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Previously Presented) A method of identifying unwanted messages, the method comprising:

inspecting a payload portion of an electronic mail message being communicated and identifying characteristics of the payload portion, the electronic mail message including an address of a recipient;

comparing the characteristics of the inspected payload portion of the electronic mail message with stored data indicating characteristics of at least one other electronic mail message that has been inspected;

based on comparison results, identifying a first security condition for the electronic mail message from among at least one of acceptable, unacceptable, and indeterminate states; and

processing the electronic mail message based on the first security condition, wherein processing the electronic mail message includes:

rejecting the electronic mail message if the first security condition associated with the electronic mail message reflects the unacceptable state;

accepting the electronic mail message if the first security condition associated with the electronic mail message reflects the acceptable state; and

if the first security condition associated with the electronic mail message reflects the indeterminate state, monitoring the electronic mail message by:

transmitting the electronic mail message based on the address of the electronic mail message;

tracking a location of the transmitted electronic mail message;

inspecting at least one other electronic mail message subsequent to transmitting the electronic mail message;

updating the stored data to indicate characteristics of the at least one other electronic mail message that has been inspected;

recategorizing the first security condition of the transmitted electronic mail message to a second security condition of the transmitted electronic mail message based on the updated stored data; and

reprocessing the transmitted electronic mail message based on the second security condition, wherein reprocessing the transmitted electronic mail message includes deleting the transmitted electronic mail message if the second security condition reflects the unacceptable state.

2. (Original) The method of claim 1 wherein the characteristics of the payload portion include information other than address information.

3. (Original) The method of claim 2 wherein the characteristics of the payload portion do not include address information.

4-5. (Cancelled).

6. (Previously Presented) The method of claim 1 wherein a security condition associated with an electronic mail message is identified as reflecting the unacceptable state when the comparison of the characteristics reveals a threshold number of messages having a shared characteristic.

7. (Previously Presented) The method of claim 6 wherein reprocessing the transmitted electronic mail message based on the second security condition includes deleting the transmitted electronic mail message if the security condition associated with the at least one other electronic mail message inspected subsequent to the transmitting the electronic mail message is identified as reflecting the unacceptable state and the at least one other electronic mail message has characteristics in common with the transmitted electronic mail message.

8. (Previously Presented) The method of claim 1 further comprising tracking the characteristics of the payload portion for comparison against characteristics of future electronic mail messages, wherein the characteristics of a new electronic mail message are compared with the characteristics of at least one electronic mail message that has been tracked.

9. (Previously Presented) The method of claim 8 wherein comparing the characteristics of the payload portion includes comparing the characteristics of the payload portion of electronic mail messages inspected with stored characteristics of other communicated electronic mail messages.

10. (Previously Presented) The method of claim 8 wherein the characteristics of the payload portion of the electronic mail message are tracked when the first security condition is identified as reflecting the indeterminate state.

11. (Previously Presented) The method of claim 10 wherein an indeterminate state is identified if the comparison of the characteristics does not itself reveal an unacceptable state, but the characteristics of the payload portion would reveal the unacceptable state in combination with similar characteristics of other electronic mail messages.

12. (Previously Presented) The method of claim 10 further comprising accepting the transmitted electronic mail message if the second security condition associated with the transmitted electronic mail message reflects the acceptable state.

13. (Cancelled).

14. (Previously Presented) The method of claim 1 wherein identifying the first security condition includes comparing the characteristics of more than one electronic mail message received by a single device.

15. (Previously Presented) The method of claim 1 wherein identifying the first security condition includes comparing the characteristics of more than one electronic mail message sent by a single device.

16-29. (Cancelled).

30. (Previously Presented) The method of claim 1 wherein recategorizing the first security condition of the transmitted electronic mail message to a second security condition of the transmitted electronic mail message includes recategorizing the first security condition of the transmitted electronic mail message to a second security condition that reflects the acceptable state.

31. (Previously Presented) The method of claim 1 wherein recategorizing the first security condition of the transmitted electronic mail message to a second security condition of the transmitted electronic mail message includes recategorizing the first security condition of the transmitted electronic mail message to a second security condition that reflects the unacceptable state.

32. (Previously Presented) The method of claim 1 wherein identifying the first security condition as reflecting the acceptable state includes identifying the first security condition as reflecting a neutral state.

33. (Previously Presented) The method of claim 1 wherein identifying the first security condition as reflecting the unacceptable state includes identifying the first security condition as reflecting a hostile state.

34. (Previously Presented) The method of claim 1 wherein recategorizing the first security condition of the transmitted electronic mail message is performed when the stored data is updated such that the security condition associated with an electronic mail message with certain characteristics would be identified as reflecting a state other than the indeterminate state

and the security condition associated with an electronic mail message with the same characteristics would have been identified as reflecting the indeterminate state prior to the update.

35. (Previously Presented) The method of claim 1 wherein recategorizing the first security condition of the transmitted electronic mail message is performed if at least one other electronic mail message inspected subsequent to transmitting the electronic mail message includes a characteristic that increases the number of electronic mail messages inspected with that characteristic above a threshold level.

36-37. (Cancelled).

38. (Previously Presented) The method of claim 1 wherein recategorizing the first security condition of the transmitted electronic mail message is performed when an administrator updates the stored data to indicate that at least one characteristic of an electronic mail message is acceptable.

39. (Previously Presented) The method of claim 1 wherein recategorizing the first security condition of the transmitted electronic mail message is performed when an administrator updates the stored data to indicate that at least one characteristic of an electronic mail message is unacceptable.

40. (Previously Presented) The method of claim 1 wherein reprocessing the transmitted electronic mail message includes removing the transmitted electronic mail message from storage if the second security condition reflects the unacceptable state.

41. (Previously Presented) The method of claim 1 wherein reprocessing the transmitted electronic mail message includes generating an alarm if the second security condition reflects the unacceptable state.

42. (Previously Presented) The method of claim 1 wherein reprocessing the transmitted electronic mail message includes continuing to track the location of the transmitted electronic mail message if the second security condition still reflects the indeterminate state.

43. (Previously Presented) The method of claim 1 wherein recategorizing the first security condition of the transmitted electronic mail message includes:

accessing the location of the electronic mail message;

retrieving the electronic mail message from the location;

inspecting the payload portion of the transmitted electronic mail message and identifying characteristics of the payload portion;

comparing the characteristics of the payload portion of the transmitted electronic mail message with the updated stored data; and

in response to comparing, identifying the second security condition from among at least one of the acceptable, unacceptable, and indeterminate states.

44. (Withdrawn) A method of determining a definitive classification of a first message, the method comprising:

comparing at least one characteristic of the first message being communicated with a set of rules used in determining classification of messages;

in response to comparing, determining whether the first message is associated with a definitive classification;

tracking the first message as a tracked message if the first message is not associated with a definitive classification; and

subsequently attempting to determine the definitive classification for the tracked message if the set of rules has been updated.

45. (Withdrawn) The method of claim 44 further comprising:

continuing to track the first message as a tracked message if determining whether the first message is associated with the definitive classification for the tracked message fails to indicate a definitive classification for the tracked message.

46. (Withdrawn) The method of claim 44 further comprising:

processing the first message based on the classification of the first message if the first message is determined to be associated with the definitive classification.

47. (Withdrawn) The method of claim 44 wherein the first message is determined to be associated with the definitive classification if a security condition associated with the first message is associated with an acceptable state.

48. (Withdrawn) The method of claim 44 wherein the first message is determined to be associated with the definitive classification if a security condition associated with the first message is associated with an unacceptable state.

49. (Withdrawn) The method of claim 44 wherein the first message is determined to be associated with the definitive classification if a security condition associated with the first message is associated with a neutral state.

50. (Withdrawn) The method of claim 44 wherein the first message is determined to be associated with the definitive classification if a security condition associated with the message is associated with a hostile state.

51. (Withdrawn) The method of claim 44 wherein the first message is not determined to be associated with the definitive classification if a security condition associated with the first message is associated with an indeterminate state.

52-54. (Canceled)

55. (New) At least one storage medium storing one or more computer programs, the one or more computer programs including instructions that, when executed, perform operations comprising:

inspecting a payload portion of an electronic mail message being communicated and identifying characteristics of the payload portion, the electronic mail message including an address of a recipient;

comparing the characteristics of the inspected payload portion of the electronic mail message with stored data indicating characteristics of at least one other electronic mail message that has been inspected;

based on comparison results, identifying a first security condition for the electronic mail message from among at least one of acceptable, unacceptable, and indeterminate states; and

processing the electronic mail message based on the first security condition, wherein processing the electronic mail message includes:

rejecting the electronic mail message if the first security condition associated with the electronic mail message reflects the unacceptable state;

accepting the electronic mail message if the first security condition associated with the electronic mail message reflects the acceptable state; and

if the first security condition associated with the electronic mail message reflects the indeterminate state, monitoring the electronic mail message by:

transmitting the electronic mail message based on the address of the electronic mail message;

tracking a location of the transmitted electronic mail message;

inspecting at least one other electronic mail message subsequent to transmitting the electronic mail message;

updating the stored data to indicate characteristics of the at least one other electronic mail message that has been inspected;

recategorizing the first security condition of the transmitted electronic mail message to a second security condition of the transmitted electronic mail message based on the updated stored data; and

reprocessing the transmitted electronic mail message based on the second security condition, wherein reprocessing the transmitted electronic mail message includes deleting the transmitted electronic mail message if the second security condition reflects the unacceptable state.

56. (New) An electronic system comprising:

at least one storage element configured to store data indicating characteristics of electronic mail messages; and

at least one processor configured to execute instructions, stored on the at least one storage element, to perform operations comprising:

inspecting a payload portion of an electronic mail message being communicated and identifying characteristics of the payload portion, the electronic mail message including an address of a recipient;

comparing the characteristics of the inspected payload portion of the electronic mail message with stored data indicating characteristics of at least one other electronic mail message that has been inspected;

based on comparison results, identifying a first security condition for the electronic mail message from among at least one of acceptable, unacceptable, and indeterminate states; and

processing the electronic mail message based on the first security condition, wherein processing the electronic mail message includes:

rejecting the electronic mail message if the first security condition associated with the electronic mail message reflects the unacceptable state;

accepting the electronic mail message if the first security condition associated with the electronic mail message reflects the acceptable state; and

if the first security condition associated with the electronic mail message reflects the indeterminate state, monitoring the electronic mail message by:

transmitting the electronic mail message based on the address of the electronic mail message;

tracking a location of the transmitted electronic mail message;

inspecting at least one other electronic mail message subsequent to transmitting the electronic mail message;

updating the stored data to indicate characteristics of the at least one other electronic mail message that has been inspected;

recategorizing the first security condition of the transmitted electronic mail message to a second security condition of the transmitted electronic mail message based on the updated stored data; and

reprocessing the transmitted electronic mail message based on the second security condition, wherein reprocessing the transmitted electronic mail message includes deleting the transmitted electronic mail message if the second security condition reflects the unacceptable state.

57. (New) An electronic system comprising:

means for inspecting a payload portion of an electronic mail message being communicated and identifying characteristics of the payload portion, the electronic mail message including an address of a recipient;

means for comparing the characteristics of the inspected payload portion of the electronic mail message with stored data indicating characteristics of at least one other electronic mail message that has been inspected;

means for, based on comparison results, identifying a first security condition for the electronic mail message from among at least one of acceptable, unacceptable, and indeterminate states; and

means for processing the electronic mail message based on the first security condition, wherein the means for processing the electronic mail message includes:

means for rejecting the electronic mail message if the first security condition associated with the electronic mail message reflects the unacceptable state;

means for accepting the electronic mail message if the first security condition associated with the electronic mail message reflects the acceptable state; and

means for, if the first security condition associated with the electronic mail message reflects the indeterminate state, monitoring the electronic mail message by:

transmitting the electronic mail message based on the address of the electronic mail message;

tracking a location of the transmitted electronic mail message;

inspecting at least one other electronic mail message subsequent to transmitting the electronic mail message;

updating the stored data to indicate characteristics of the at least one other electronic mail message that has been inspected;

recategorizing the first security condition of the transmitted electronic mail message to a second security condition of the transmitted electronic mail message based on the updated stored data; and

reprocessing the transmitted electronic mail message based on the second security condition, wherein reprocessing the transmitted electronic mail message includes deleting the transmitted electronic mail message if the second security condition reflects the unacceptable state.